**Temat: Uprawnienia w Linuxie.**

**chmod** (*change mode* – zmiana atrybutu) – polecenie zmiany zezwoleń dostępu do plików w systemach [uniksowych](https://pl.wikipedia.org/wiki/Unix).

**Opis klas użytkowników**

* **u** – użytkownik ( ***u****ser*)
* **g** – grupa ( ***g****roup*)
* **o** – inni ( ***o****thers*)
* **a** – wszyscy (***a****ll*)

**Uprawnienia**

Istnieje kilka sposobów zapisu praw do danego pliku. Najpopularniejszymi są: system numeryczny, oraz literowy. Numerycznie chmod przyjmuje odpowiednią wartość potęgi [dwójki](https://pl.wikipedia.org/wiki/2_%28liczba%29) dla każdego typu akcji (zapisu, odczytu, uruchomienia).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Typ zapisu** | **Prawo odczytu** | **Prawo zapisu** | **Prawo uruchomienia** | **Specjalne prawo uruchomienia** | [**UID**](https://pl.wikipedia.org/wiki/UID)**/**[**GID**](https://pl.wikipedia.org/wiki/GID) | [**sticky bit**](https://pl.wikipedia.org/wiki/Sticky_bit) |
| Potęga dwójki | 22 | 21 | 20 |  |  |  |
| Wartość w [ósemkowym systemie liczbowym](https://pl.wikipedia.org/wiki/%C3%93semkowy_system_liczbowy) | 4 | 2 | 1 |  |  |  |
| Znak | r ([ang](https://pl.wikipedia.org/wiki/J%C4%99zyk_angielski). ***r****ead*) | w ([ang](https://pl.wikipedia.org/wiki/J%C4%99zyk_angielski). ***w****rite*) | x ([ang](https://pl.wikipedia.org/wiki/J%C4%99zyk_angielski). *e****x****ecute*) | X | s | t |

Aby zapisać uprawnienia w systemie numerycznym należy dodać liczby odpowiadające uprawnieniom, które chcemy przyznać. Należy tak postąpić osobno dla właściciela, grupy oraz innych, np. właściciel – wszystkie prawa, grupa – odczyt, inni – brak należy zapisać jako: 740.

Aby zapisać uprawnienia w systemie znakowym należy wpisać znak **u**, **g**, **o** lub **a** następnie znak:

* **+** jeżeli chcemy dodać uprawnienia,
* **–** jeżeli chcemy odebrać uprawnienia,
* **=** jeżeli chcemy zmienić uprawnienia (tzn. przypisać takie, jakie podamy),

a następnie odpowiednie oznaczenia z tabeli.

Po przecinku można dopisać kolejne uprawnienia (np. u=rwx,g+rw,o-r wprowadza następujące zmiany:

* dla właściciela – ustawiono odczyt, zapis oraz wykonanie, ale to ostatnie tylko wtedy jeżeli ono już jest ustawione, w innych plikach pozostanie wyłączone,
* dla grupy – dodano odczyt i zapis,
* dla innych – odebrano odczyt.)

By zobaczyć jakie prawa ma dany plik, lub katalog wystarczy użyć polecenia [ls](https://pl.wikipedia.org/wiki/Ls) z (opcją *-l*).

$ ls -l

razem 2844

drw-r--r-- 1 user admin 4096 maj 28 16:38 folder1/

drwxrwxr-x 6 user admin 4096 maj 25 19:18 folder2/

drw-rw-r-- 1 user admin 4096 maj 26 15:56 folder3/

**Tabela z interpretacją kodów ósemkowych**

|  |  |  |
| --- | --- | --- |
| **Cyfra** | **Prawa** | **Litera** |
| 0 | Brak praw | --- |
| 1 | Wykonywanie | --x |
| 2 | Zapis | -w- |
| 3 | Zapis i wykonanie | -wx |
| 4 | Odczyt | r-- |
| 5 | Odczyt i wykonanie | r-x |
| 6 | Odczyt i zapis | rw- |
| 7 | Odczyt, zapis i wykonanie | rwx |

**Przykłady uprawnień**

|  |  |  |
| --- | --- | --- |
| **Prawa dostępu** | **Wartość liczbowa** | **Opis** |
| -rw------- | 600 | Tylko właściciel ma prawo do odczytu i zapisu. |
| -rw-r--r-- | 644 | Właściciel ma prawo do zapisu i odczytu, a reszta tylko prawo odczytu. |
| -rw-rw-rw- | 666 | Wszyscy mają prawo do odczytu i zapisu. |
| -rwx------ | 700 | Tylko właściciel ma prawo do odczytu, zapisu, uruchomienia. |
| -rwxr-xr-x | 755 | Właściciel ma wszystkie prawa do pliku, reszta tylko prawo do odczytu i uruchomienia. |
| -rwxrwxrwx | 777 | xxxxxxxx |
| -rwx--x--x | 711 | Wszystkie prawa ma właściciel, reszta tylko prawo uruchomienia. |
| drwx------ | +++ | Właściciel katalogu ma pełne prawa do niego (katalogi mają literkę 'd' na początku zamiast '-') |
| drwxr--r-- | 744 | Właściciel ma pełne prawa do katalogu, reszta ma prawo do odczytu. |
| -rwsr-xr-x | 4755 | Właściciel ma pełne prawa do pliku, grupa ma prawa odczytu i wykonania, reszta ma prawo odczytu i uruchamiania. Plik ma [atrybut SUID](https://pl.wikipedia.org/wiki/Setuid) (pierwsza cyfra w opcjach jest równa 4). Oznacza to, że plik wykonywalny, np. wywołuje proces i oddaje mu kontrole nad wykonaniem zadania. Bez opcji SUID proces działa z uprawnieniami użytkownika, który uruchomił plik, co czasami może powodować niewykonanie zadania, gdyż użytkownik nie miał dostatecznych uprawnień. Z opcją SUID proces pobiera uprawnienia właściciela pliku, najczęściej roota. Polecenie ping i uprawnienia do pliku wykonywalnego są przykładem wykorzystania tej opcji. |

**Przykłady użycia**

* $ chmod a+w plik.txt — nadaje wszystkim uprawnienia do zmiany 'plik.txt',
* $ chmod o-x plik.txt — usuwa możliwość wykonywania 'plik.txt' przez pozostałych użytkowników,
* $ chmod go=rx plik.txt — grupa oraz pozostali użytkownicy będą mogli tylko czytać i wykonywać.
* $ chmod -R 777 /home/user — wszyscy będą mogli zmieniać zawartość katalogu /home/user oraz jego podkatalogów, jak też czytać go i wykonywać zawarte w nim pliki

W Linuksie istnieje specjalne prawo dostępu zwane **SUID** (SetUID). Normalnie program może być uruchomiony przez użytkownika który jest jego właścicielem, ale są sytuacje gdy program ( należący do *roota* ) musi być uruchomiony przez osobę, do której nie należy (np.*ping* należy do *roota* a mimo tego, może być uruchomiony przez innych użytkowników). Aby umożliwić pozostałym użytkownikom korzystanie z takich programów trzeba nadać im specjalny atrybut **SUID**. Aby to zrobić należy liczbę określającą prawa dostępu poprzedzić cyfrą **4**, przykład:

chmod 4755 /bin/ping

lub w metodzie symbolicznej użyj opcji **s**:

chmod +s /bin/ping

Prawa czytania, pisania i wykonania w takich plikach widoczne są jako **rws** a nie **rwx**
Bardzo dobrym narzędziem do wykonania opisanych tu operacji jest MidnightCommander (MC).